Memorandum

U.S. Department
of Transportation

Federal Aviation
Administration

Subject:	INFORMATION: Guidance for the Certification of Honeywell Primus Epic Systems	Date:	May 30, 2003
From:	Manager, Transport Airplane Directorate, ANM-100	Reply to Attn. of:	Connie Beane, ANM-02-113-016
To:	See Distribution	Regulatory Reference:	§ 25.1301, § 25.1309, AC 25.1309-1A

PURPOSE

The purpose of this memorandum is to establish the Federal Aviation Administration (FAA) Transport Airplane Directorate (TAD) guidance for the certification of Honeywell Primus Epic® (referred to as Epic from here forward in this document) Systems.

SCOPE

This policy memorandum provides guidance on the following issues associated with Epic systems:

1. Roles and Responsibilities
2. Airplane Level Safety Assessment
3. Configuration Management
4. Electronic Identification Part Marking
5. Software Design Assurance Considerations
6. Hardware Assurance
7. Human Factors
8. Certification Plan

BACKGROUND

In the past several years, new aircraft designs have introduced new technologies. These technologies are being combined and used in novel ways and may represent significant challenges with respect to the acceptability of the flight crew interfaces and aircraft airworthiness.

Epic systems are an avionics suite consisting of single or multiple racks and cabinets with circuit cards/modules that are installed in slots in the cabinets. Each module can contain one or more functions. Each cabinet's configuration can vary in that the number of modules installed in each cabinet can vary, the functions loaded into the modules can vary, and there can be multiple racks and cabinets installed on the aircraft. The functionality of the system's modules is determined by the software loaded into the modules. All the software on these modules can be field-loaded, that is, loaded into the Epic modules without removing the equipment from the aircraft.

CURRENT REGULATORY AND ADVISORY MATERIAL

See Appendix A for a listing of applicable related guidance material.

POLICY STATEMENTS

1. Roles and Responsibilities

It is important that all parties involved in an Epic certification project, whether it be a type certificate (TC), amended type certificate (ATC), supplemental type certificate (STC) or amended supplemental type certificate (ASTC) project, understand their roles and responsibilities. There are four primary roles or stakeholders in the development, verification, certification, installation, and validation of Epic systems.

a. Honeywell – developer and supplier of the Epic systems' racks, cabinets and modules, including many of the hardware components and software applications that are field-loaded and provide the Epic system functions; and developer and supplier of other non-Epic systems to be installed on the aircraft.

b. Third party suppliers and manufacturers – may provide additional modules and software applications to be hosted in the Epic system.

c. TC, ATC, STC, ASTC applicant – responsible for the entire certification program and integration, installation and validation of the Epic system on the aircraft.

d. Certification authority – government agency or organization responsible for finding compliance to the applicable sections of 14 CFR.

The following identifies basic responsibilities of the four primary stakeholders:

a. Honeywell –

- Design and build the common (basic) hardware elements.
- Develop the common software and application specific software to support the applicants' aircraft programs.
- Provide Epic system-level verification and validation data to support applicants' aircraft programs.
- Coordinate certification issues regarding the common and application specific safety, human factors, electrical, hardware and software and Epic system compliance with regulations with the certification authority.

b. Third party suppliers–

- Develop hardware and software applications to be hosted in Epic systems.
- Obtain technical standard order authorization (TSOA) for functions, if desired, necessary, and available.
- Provide module/card level verification and validation data to support integration in the Epic system.
- Provide other integration verification and validation data, as necessary to support certification of the installation.

c. TC, ATC, STC, ASTC applicant –

- Perform aircraft level safety assessment of their specific configuration of the Epic system and other aircraft equipment.
- Ensure Epic system components are developed, verified and validated to the appropriate assurance levels to support the safety assessment.
- Integrate Epic system components into the aircraft.
- Integrate third party elements (hardware and/or software) into the Epic system.
- Perform aircraft level validation and verification to validate the safety assessment.
- Determine appropriate environmental conditions.
- Perform environmental qualification testing (EQT) and ensure previously conducted EQT (conducted by Honeywell or third party suppliers) is appropriate for the aircraft installation and operating environment.
- Show compliance with all applicable regulations.
- Perform aircraft integration test, ground test and flight test to support certification and operational approval.

d. Certification Authority –

- Establish certification basis.
- Resolve regulatory issues associated with each Epic system aircraft program.
- Find compliance to applicable sections of 14 CFR.
- Issue applicable TC, ATC, STC, ASTC.

2. Airplane Level Safety Assessment

The Epic systems can combine many functions into a common avionics suite, that have historically been installed in functionally and physically separate systems. In Epic system architectures, electrical power, computing hardware, memory, data busses, physical location, etc., could all be shared for multiple functions, some of which have related functions and some of which have little or no relationship. This brings up several concerns:

a. Possible interference of critical systems, such as fly-by-wire flight controls or autopilot functions, by functions of lower criticality.
b. Failure conditions (either single or multiple) which could affect multiple functions, thereby possibly increasing the hazard effect of failures, causing increased flight deck workloads and dramatically increasing the "confusion factor" and stress level of the flight crew while attempting to determine the nature of the failures and the correct flight crew response.
c. The system response to failures may become less deterministic.

To demonstrate that the airplane complies with § 25.1309, the applicant should perform an airplane level safety assessment that addresses Epic systems' integration issues. This airplane level safety assessment should be supplemented by the safety assessments of the individual systems and functions. The focus of the airplane level safety assessment should be the identification of the cross-functional effects of single and/or multiple failure combinations. Cascading or common cause failures, and fault propagation effects, if they exist, should be identified and mitigated by the Epic system architecture and features. Detailed guidance for conducting safety assessments of complex, highly integrated systems is provided in SAE documents ARP4754 and ARP4761.

The guidance below discusses the data that the FAA may find necessary to determine that the safety objectives, at the airplane level, have been assured by the applicant. If a specific Epic system configuration does not have a high level of integration (e.g., critical systems such as flight control functions are not integrated into the Epic system), the scope of this guidance may be reduced accordingly.

a. The applicant should identify all airplane level functions that are integrated in the Epic system. Because Epic systems are highly adaptable, the airplane level functions that are integrated into the Epic system on a specific airplane program vary depending on the chosen configuration. The safety-critical airplane level functions could be grouped into four generic categories:

   - Control airplane on the ground.
   - Control airplane in flight.
   - Provide a livable cabin environment.
   - Protection against common threats such as:
     - Fire.
     - Uncontained engine and APU rotorburst.

- Engine bladeout due to vibration.
- Tire burst.
- Thrown tire tread.
- Wheel rim release.
- Runway debris.
- Bird strike.
- HIRF and lightning strikes.
- Duct rupture.
- Explosion (sabotage).
- Release of stored energy (batteries, accumulators, pressure bottles).

Each of the above generic categories can be expanded to the functional level. For example, “Control airplane in flight” is a grouping of airplane level functions such as:

- Control pitch.
- Control yaw.
- Control roll.
- Control lift and /drag.
- Control thrust.
- Provide autoflight.
- Display primary flight data.
- Navigate.
- Communicate.

b. The applicant should identify the specific configuration of the airplane installation, including interfaces with airplane systems not implemented in Epic and how each airplane level function is implemented.

Each airplane level function may be implemented by one or more systems. Similarly, an individual system may provide for more than one of those functions. A matrix (see example below) showing how functions are provided is a simple and powerful tool to determine, at a glance, the separation of systems and functions as well as any potential impact of common cause/cascade failures. For example, the Control Airplane On The Ground function is provided by the landing gear (nose steering, brakes), the flight control surfaces (rudder, spoilers), thrust reversers. The applicant should identify which of these systems are controlled by (or communicate with) the Epic system. The following information should also be submitted by the applicant:

- A block diagram showing how the Epic system interfaces with other systems.
- A listing of how the flight crew interfaces with the airplane systems.
- A description of how functions are installed and partitioned in the specific Epic system architecture.
- List of complex electronic hardware components, software applications and their functions.

AIRPLANE-LEVEL FUNCTION AND SYSTEM INTEGRATION MATRIX (Notional)

	Implemented by			
A/C Level Functions	System A	System B	…	System Z
F1	✓			
F2		✓		✓
…				
Fh			✓	
Fn	✓			

This matrix illustrates:

- The system configuration with respect to intended functions.
- If a failure of a single system may impact multiple functions (system A and functions F1, Fn).
- The availability of a function may be provided by multiple systems (e.g., F2 implemented in systems B and Z). System redundancy or backup mechanisms would be apparent (for example, a "direct mode" in the flight control system that bypasses the "normal mode" that resides in the Epic system.)

c. The applicant's airplane-level safety assessment process should ensure that the required level of safety is achieved. Safety assessment at the airplane level is inherently an integration issue. Integration, in turn, is a process issue. Therefore, the FAA needs visibility of the applicant's airplane-level safety assessment process leading to the assurance that the airplane safety objectives will be met. In evaluating such a process, it is important to identify the methods for addressing cross-functional effects of failures. The process should include a systematic approach for selecting:

- The airplane functions to analyze.
- The systems that implement those functions.
- The types of failures of those systems.

The means and frequency of providing the visibility should be mutually agreed to between the FAA and the applicant. The process and plans for performing the airplane level safety assessment should be presented to the FAA for review and comment as early as possible in the project.

d. The applicant should provide, for FAA review, an airplane level functional hazard assessment (FHA), and propose a method for assigning assurance levels to system, software, and hardware components.

ARP4761 describes how an airplane level FHA may be performed. It should be noted that some applicants have erroneously considered a <u>system</u> to be the airplane level <u>function</u> and then performed the safety assessment only at the system level, thus failing to do the assessment at the airplane level. An example to clarify this point: an airplane level function is “Navigate” and is not “Display Navigation Data”. A functional hazard associated with the “Navigate” function may be the inability to find an airport due to loss of heading and position information, where loss of the displays could be a system failure leading to the above hazard.

The safety objective associated with each failure should be identified by the applicant and agreed to with the FAA. Determination of the appropriate system development assurance levels, hardware design assurance levels, and software levels should be the result of a preliminary system safety assessment, and not a predicated assignment.

e. A detailed airplane level safety assessment should be provided to and agreed upon by the certification authority. A summary of the all catastrophic, hazardous/severe-major, and major system failure conditions should be provided to the FAA for review. Items of specific interest include:

- Single failures leading to the top level hazards categories.
- Failures leading to top-level hazard events as a result of multiple failures of less severity.
- Cascading and common mode failures.
- Effects of latent failures.
- Latent failures that could leave the airplane one failure away from a catastrophic event.
- Effects of fault propagation, if any, through the Epic channels.
- Environmental effects (HIRF, lightning, temperature, moisture, vibration, etc…).
- Effects of possible flight crew and maintenance crew errors (these errors are not to be incorporated in fault trees, however).
- The number of failure conditions having catastrophic effects. If the number is very high (more than 100), the reliability of the airplane from the cumulative risk standpoint is questionable. Note that the 10^{-9}/flight-hour probability criterion was developed from the assumption that the cumulative risk would not exceed 10^{-7}/ flight-hour for fatal accidents to which system failures were contributing factors.
- Dispatch Configurations - Performing the safety assessment with all systems fully functional (full up configuration) does not accurately represent the condition of a typical in-service airplane. A fault tolerant system enables the operators to defer maintenance and dispatch with some failure present. As part of the MMEL/MEL process, the FAA should evaluate each proposed dispatched configuration in light of the same issues discussed above, with the exception of the cumulative risk assessment. Of particular interest is the reliability and integrity requirements for the residual system configurations. When the airplane operates at a reduced degraded functionality or capability, there should be adequate assurance of the integrity and reliability of the residual airplane systems for the duration of the exposure period until the equipment is repaired (i.e., should a higher design assurance levels be required of specific components if certain dispatch configurations are allowed?).

f. Non-essential Functions - The safety analysis should provide an assurance that non-essential functions or systems (such as cabin entertainment) do not interfere with functions necessary for normal flight operations or when failures occur. The applicant is not required to perform airplane-level safety assessments of non-essential functions.

g. Validation and Verification of Fail Safe Designs - The applicant should be expected to provide a comprehensive airplane validation and verification program that consists of:

- Actions to validate critical assumptions made in the safety assessment (e.g., assumptions that the flight crew would correctly perform certain mitigating action in response to failures).
- Actions that verify the intended functions of the airplane.
- Actions that verify that all integrated systems do not perform unintended functions.
- Pass/fail criteria for each validation and verification action. These pass/fail criteria should contain adequate margins to allow for implementing Epic core components on the applicant's various airplane models. Configuration sensitivity within each airplane model should also be considered.
- Actions to measure the airplane's and flight crew's responses to critical failure modes.

3. Configuration Management

An Epic system may contain many hardware components and software applications, with many valid configurations approved for each airplane. Techniques are necessary to effectively manage and utilize the Epic system architecture to safely provide system attributes such as:

a. Hosting of multiple software applications on a single Epic module (card and/or processor with shared resources).

b. Production and distribution of hardware components that are not loaded with their specific software functional applications ("non-functional" or "brain dead" hardware).

c. Allowing electronic part numbering for software, without the need to physically mark hardware with the software part number. See FAA notices on field-loadable software.

d. Allowing the electronic display of hardware component and software application identifications for the system.

e. Allowing the field-loading of hardware modules with software applications for efficient maintenance and incorporation of approved design changes.

f. Allowing the stocking of generic non-configured hardware modules for maintenance. A non-configured hardware module is one that does not contain functional specific software applications.

g. Allowing the field-loading of all Epic system software applications from a single medium.

h. Allowing the use of loadable configuration files and registries that define the specific Epic system and airplane configurations; define which Epic hardware modules and memory devices that software applications are loaded into, and procedures needed to validate an Epic system field-load.

A robust automated configuration management and validation scheme is required to enable the safe operation and maintenance of an Epic system. It should have the following characteristics:

a. Multiple means of identifying invalid configurations of Epic system components and software loads. Because of the potential system complexity, configuration control using hardware and software part numbers and modification status alone is not considered sufficient for Epic systems.

b. Verification of hardware and software identifiers for the integrated system and for each Epic module and module location.

c. Verification that software applications and hardware components of the system are correct for the airplane they are installed on and compatible with each other.

d. Detection of invalid configurations prior to each flight, annunciated to the flight crew. An invalid configuration means the airplane cannot be dispatched.

Simple Epic systems that do not include field-loadable software may not need an automated configuration management and validation scheme if the manufacturer provides mechanical interlocks, such as keyed connectors, that would prevent the incorrect assembly, configuration or installation of the modules in the cabinet.

If individual hardware components require interfaces to the airplane or other equipment by means of a mechanical connector(s), the applicant should be able to validate that each such interface, by either mechanical means or automatic electronic monitoring of interface will either prevent an incorrect connection or that the occurrence of an incorrect connection will be positively detected prior to each flight.

When a software change is made, whether it is major or minor, a part number revision should occur and the configuration management records and airplane configuration data should be updated.

Applicants should develop a procedure to ensure that the correct software is loaded on an airplane. There should be more than one method to verify that correct software has been loaded.

All changes made to an installed Epic system should be approved under a certification process (TC/ATC/STC/ASTC). All changes should result in a change to the configuration identification of the Epic system at the airplane installation level. An engineering evaluation of each change should be completed by the TC/ATC/STC/ASTC holder prior to implementing the change.

4. Electronic Identification Part Marking

Epic systems, as noted previously, are assembled from common hardware modules and cabinets and may not be loaded with operational software when installed on the airplane. Therefore, the traditional method of mechanically marking part numbers and revision levels on the equipment nameplate may not be practical. However, a means should be provided to quickly and accurately ascertain the part numbers of both the Epic system hardware and software while all Epic components, including software, are installed on the airplane.

Identification of Epic software applications should be implemented by electronic means, unless the automated configuration management system is unnecessary because the Epic system does not support field-loadable software. This method of marking consists of the process of identifying software components by electronically embedding the identification within the hardware component itself (using software), rather than marking it on the equipment nameplate.

Electronic software part numbers and version should be verifiable through some kind of electronic query, on an electronic display or a carry-on unit. Software part number configuration faults must be displayed and annunciated.

14 CFR Section 21.607 requires TSO'd equipment to be permanently and legibly marked with specific information. Compliance to §21.607 can be demonstrated for software when the information required is provided by an electronic identification scheme which is stored in non-volatile memory. The electronic identification system should be verifiable on-board the airplane and provide the specific information for all TSO's being integrated. Electronic identification may also provide software application and hardware component revision status information which can be used to demonstrate conformity to the airplane type design configuration. Information identifying the location of each hardware component should be included in the electronic identification since configuration control is dependent on the specific location of each hardware component and software application within an Epic system cabinet. The electronic identification information is an acceptable alternative to physical verification of hardware part number and revision status instead of verifying data plates on each hardware component. Electronic identification does not replace hardware and software element conformity inspections, which determine that the elements are produced and installed in conformity to type design. A duplication process which archives the Epic software and hardware element identifications and revision status off-board the airplane is required.

5. Software Design Assurance Considerations

All software to be installed in the Epic system should be developed in accordance with AC 20-115B, FAA software notices applicable to cross-FAR applications, TAD software issue papers, as applicable, and RTCA document DO-178B (or another acceptable means of compliance for software approval). Some considerations and concerns are as follows:

a. Software levels for Epic software applications should be determined by the appropriate airplane-level and system safety assessments and any additional requirements, such as those specified by functional TSO requirements. In Appendix C, there is a generic TAD issue paper for this subject that should be applied to all Epic system airplane programs.

b. Field-Loadable Software - All software applications intended to be installed in the Epic system are field-loadable. This is software which can be loaded into the Epic system without removal of the installed system components from the airplane. There are two FAA notices, N8110.93, Guidelines for the Approval of Field-Loadable Software by Finding Identicality Through the Parts Manufacturer Approval Process and N8110.95, Guidelines for the Approval of Field-Loadable Software, related to this subject that should be applied to all Epic system airplane programs. To obtain approval for this capability, the following should also be addressed:

- Assurance that redundant functions have the same software configuration, unless intermixing of different configurations are supported by the safety assessment and have been verified and validated for the airplane type design.
- Assurance that software loading procedures will verify that the software loaded is the approved software for that airplane and Epic system's approved configuration, that it has not been corrupted during the load, that it is loaded into the appropriate module's memory, and that all loading errors, configuration mismatches, and anomalies are detected, annunciated to the flight crew or maintenance personnel, and corrected before the airplane can be dispatched.
- Assurance that loading, from all mediums being used (diskette, CD-ROM, Network, etc.), comply with these guidelines.
- Capability to verify the software part numbers with on-board equipment, carry-on equipment or other appropriate means.
- Loading protection mechanisms to inhibit loading during flight.
- An acceptable loading procedure, including actions to be taken in the event of an unsuccessful load.

c. User-modifiable software may be available for some Epic system configurations. This is software that may be modified by the airline/operator. There is an FAA notice, 8110.94, Guidelines for the Approval of Airborne Systems and Equipment Containing User-Modifiable Software, and TAD generic issue paper (see Appendix C) related to this subject that should be applied to all Epic system airplane programs.

d. A change impact analysis is needed for any software being used from previously developed and approved baselines which needs to be modified to function in the current installation. There is an FAA notice, 8110.85, Guidelines for the Oversight of Software Change Impact Analyses used to Classify Software Changes as Major or Minor, related to this subject that should be applied to all Epic system airplane programs. If Epic hardware components will be modified or changed in another installation, the hardware components' impact on the software should also be determined and appropriate re-verification conducted, in addition to performing, if necessary, additional environmental qualification testing, to ensure continued operational safety.

e. Software changes from one airplane installation to another need to be identified. Appendix B contains a list of the software applications expected to be installed in Epic systems. This list identifies software that will likely change from one airplane configuration to another and indicates whether the changes are considered significant. It is important that these areas be identified and the changes analyzed to determine the impact on the previously approved software. See item d above for guidance on change impact analyses.

f. Commercial off-the-shelf (COTS) software may be used in an Epic system. Typical functions may be library functions provided with compiler products, operating system software, supporting processes, etc. In Appendix C, there is a TAD generic issue paper related to this subject that should be applied to all Epic system airplane programs.

g. Assembly branch coverage (ABC) instead of modified condition decision coverage (MC/DC) may be an acceptable alternative, subject to certain limitations. There are certain design and coding rules, language restrictions, and limitations that should be applied to any development proposing to use ABC instead of MC/DC. An issue paper should be written to address the following:

- Provide assurance that test cases are generated from the requirements.
- Provide details of grammar rules, coding restrictions and limitations, compiler restrictions and limitations, complexity limitations, etc. that are necessary to ensure that ABC will provide equivalent structural coverage as MC/DC for Level A software components.
- Provide verification that the ABC grammar rules and coding, compiler and complexity restrictions and limitations are adhered to for all Level A code.
- Provide data that substantiates that the compiler behaves as assumed by the ABC approach (e.g., short-circuit behavior, compiler assumptions, compiler options and optimizations, etc.).
- All rules, restrictions and limitations should be presented to the FAA ACO to ensure their concurrence with the approach and should be included in the appropriate software planning, standards, and/or development documents.
- Provide documentation that substantiates that the results that are achieved from the Assembly Branch Coverage (ABC) method provide equivalent coverage as the results that would have been achieved using Modified Condition Decision Coverage (MC/DC).

- Describe the process for resolving issues found at the object code level (e.g., how object code can be mapped to the requirements in order to address coverage resolution issues).
- Provide complexity and architecture limitations for which ABC is applicable (e.g., number of nested "ifs", number of conditions in a decision, nested function calls, etc.), and include these limitations in software planning, standards, and development documents.

h. C++ programming language and other "object-oriented" languages have certain features and capabilities that, if not properly controlled, could result in software applications that are not configurable, non-deterministic, and very difficult to verify. An issue paper should be written to address the following:

- *Dead/Deactivated Code:* Several variations of this can occur in object-oriented systems. A few are: (a) classes in a library not used; (b) methods (functions) of a class not called in a particular application; (c) methods (functions) of an (abstract) class overridden in all subclasses; or (d) attributes of a class not accessed in a particular application.

- *Dynamic Binding/Dispatch:* The matching of calls to methods (functions) at run-time as opposed to compile-time or link-time. This results from a polymorphic call. A related issue is implicit type conversions performed dynamically to support the call. There are a number of concerns regarding the use of dynamic binding/dispatch in airborne software:

  – It complicates the flow analysis and structural coverage analysis;
  – It can lead to complex and error-prone code;
  – It can complicate source to object code traceability;
  – The matching of calls to methods can be difficult, if implicit type conversion is used; and
  – The behavior of the compiler may become non-deterministic.

- *Encapsulation:* Separation of the external (public) and internal (private) aspects of a class and its objects. Generally, the external aspects are known as the interface, while the internal aspects are known as the implementation. Clients of a class may only have access to the interface of the objects of that class and not to the internal aspects (also known as data hiding, information hiding). The concerns of encapsulation in airborne systems are:

  – The programmer may not realize unintended functionality of the class, if class features, potential side effects, pre-conditions, and post-conditions are not well-documented;

  – Traceability and configuration control of classes may become difficult to manage; and

  - Structural coverage may be difficult to obtain.

- *Inheritance:* A mechanism whereby a class is defined in terms of others (its parents), adding the features of its parents to its own. A class may have a single parent (single inheritance) or multiple parents (multiple inheritance). Either the interface, or the interface and implementation can be inherited. Where multiple inheritance is allowed, repeated inheritance is a possibility (two or more parents have a common ancestor in the class hierarchy). Multiple inheritance is particularly a concern in airborne systems. It can lead to overly complex and potentially unpredictable interactions between classes.

- *Polymorphism:* The ability of a name in software text to denote, at run-time, one or more possible entities, such as a function, a variable or an operator. For example, given the text: *f(x)*, which *f()* to call may be dependent on which class *x* belongs to, and *x* may belong to multiple classes, depending on the run-time state of the system. Polymorphism is generally supported by dynamic binding/dispatch. The concern with polymorphism and function overloading in airborne systems is the potential for ambiguity, which might lead to coding error and poor configuration management.

i. Database validation – Honeywell and other Epic system software developers may propose to use databases, configuration files, and airplane personality modules that define the functionality, “active” and “deactive” software, and configuration of the system. Typically, databases (except navigation and terrain/obstacle databases) are considered part of the software application, and should comply with the software guidance of RTCA document DO-178B to the same level as the software applications that use these databases. However, an issue paper is being developed on databases, including navigation and terrain/obstacle databases, that will be added to this guidance when available.

6. Hardware Assurance

Programmed Logic Devices

Although not typically considered software, Epic system components will likely use complex programmed logic devices (PLDs), such as field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), etc. In Appendix C, there is a TAD generic issue paper on this subject that states that the applicant (or their developer) should have structured, rigorous processes in place that provide design assurance for these devices commensurate with the “criticality” of the system, function and/or component. The issue paper provides some guidance and identifies some of the type design data for these components. The issue paper refers to RTCA DO-254 as guidance for acceptable means of compliance for these hardware devices. For Epic system components containing such devices, the guidance of DO-254 and the TAD issue paper should be applied to each Epic system and installation.

7. Human Factors

Cursor Control Devices

There is only limited experience with in-flight use of cursor control devices (CCD) on civilian transport category airplanes. That experience is restricted to use of a touchpad CCD for a small set of non-required functions. An Epic system, on the other hand, may employ several types of CCDs (e.g., trackballs, joysticks, touchpads, thumb-operated force-rate transducers, etc.) for a variety of select and control functions. This may involve the use of the CCDs during operational scenarios involving manual flight, emergencies, multiple failures, turbulence, vibration from sustained engine imbalance (blade-out), etc. In some situations, the pilots will be expected to use the CCD to select displays, position the cursor, select from menus, and navigate through menu trees to access control functions.

Another concern is the failure of a single CCD, which may disrupt the normal flow of crew tasks. The tasks on the flight deck are normally allocated based on which pilot is flying the airplane. As tasks are performed, some will be accomplished by the Pilot Flying (PF), while others will be accomplished by the Pilot Not Flying (PNF). In conventional airplane flight deck designs, the controls for such tasks are in locations that are immediately accessible to both pilots, such as the overhead panel or center pedestal. In the some Epic designs, the pilot with a failed CCD will be unable to use the other pilot's CCD. The failure of a CCD may result in an unacceptable disruption of the normal allocation of tasks and crew workload. For example, tasks that are normally allocated to one pilot, may need to be done by the other pilot using the remaining functional CCD.

Considering the constraints of flight crew workload per § 25.1523, the control design requirements of §§ 25.771(a). and 25.777(a), the environmental conditions specified in § 25.771(e), and the general design requirements in §§ 25.1301(a) and 25.1309(b) and (d), compliance for CCDs should address the following:

a. To show compliance with §§ 25.777(a) and 25.1523, the applicant should demonstrate that the pilots can conveniently access required control functions in all expected flight operations scenarios, without unacceptable disruption of airplane control, crew task performance, and Crew Resource Management (CRM). Since not all possible operational scenarios can be evaluated, the applicant should develop a set of worst case scenarios for evaluation and detailed procedures for evaluation (e.g. analysis, test, demonstration). A comparison to conventional controls should be carried out as part of this evaluation, in order to determine if the use of CCDs results in an increase in flight crew workload or task performance timelines. The evaluation plan should show how each of the factors identified in 14 CFR part 25 Appendix D will be evaluated. Operation of the CCD with both the dominant and non-dominant hand should be included in the evaluations. Operation during manual flight should be evaluated. Additionally, experience has shown that control-display response lag (i.e., time delay between movement of the control on the CCD and response of the cursor on the display) and control gain characteristics can be critical in the acceptability of a CCD. Usability testing should therefore accurately replicate the response lag and control gain characteristics that will be present in the actual airplane.

In some cases, the flight deck designs provide alternative methods for accomplishing tasks that would normally be done using the CCDs. However, it is the FAA's opinion that, due to possible novel aspects of the Epic system crew interface designs, the CCDs are intended to be the primary means for many of the pilots' communication, navigation, and situation awareness tasks. Additionally, the FAA believes that the CCD interface will be very compelling and many pilots will attempt to use it, even if alternative, more efficient control strategies are available. Therefore, if extensive use of these alternative control strategies is necessary in order to meet the requirements of § 25.1523 in expected operations, it may be determined that the use of the CCD results in a level of workload that is unacceptable for the proposed minimum crew. The applicant should document and explain those cases in which use of the CCD is not recommended.

b. To show compliance with § 25.771(e), it is the FAA position that currently available analytical techniques are inadequate. Therefore, the applicant should show by test and/or demonstration in representative motion environment(s) that the CCD is acceptable for controlling all functions that pilots will access using the CCD during these conditions. In addition to turbulence, vibration due to the loss of a fan blade and the subsequent damage to other rotating parts of the fan and engine should be considered in the definition of the motion environment. The use of laboratory "shaker tables" have been shown to be useful for testing the usability of the CCD during sustained vibration conditions which cannot be safely demonstrated in flight.

c. To show compliance with § 25.1309(b) and (d), the applicant should conduct an airplane-level safety assessment to determine the hazards and failure conditions associated with the failure of one and of both CCDs. The applicant should address the independence of the two CCDs (i.e., vulnerability to common cause failures), and the combined effects of the loss of CCD control of multiple systems and functions. The applicant should demonstrate that the failure of either CCD does not unacceptably disrupt operation of the airplane (i.e., the allocation and performance of pilot tasks) in normal and emergency conditions. The failure condition classifications described in AC 25.1309-1A can be used to assess the severity of the effect on the airplane and on flight crew operations of the loss or malfunction of a single CCD or the loss or malfunction of both CCDs, either by themselves or in combination with other failures. In conducting the safety assessment, the conditions that could result in the failure or anomalous behavior of a CCD should include fluid contamination, unless it can be shown that spills of fluids expected to be present in the flight deck (e.g., beverages, food, etc.) will not result in CCD failure, anomalous behavior, or degraded usability. The safety assessment should also include common mode failures such as physical damage, HIRF, lightning, fire, and electrical faults.

Pilot Flying vs. Pilot Not Flying

Several proposed Epic systems configurations use display arrangements that are different for the Pilot Flying (PF) and the Pilot Not Flying (PNF). This necessitates "informing" the display system which pilot is flying by pushing a button. In all of the designs reviewed to-date, selecting the "PF" button will cause the flight director to drop the current flight modes (e.g., LNAV, PROF/VNAV, LVL CHG) and change to its default modes (e.g., ALT HOLD, HDG HOLD). Thus, a task that is necessary to deal with display management will result in changes in flight guidance modes. If pilots fail to reengage the desired modes for this undesirable nuisance mode change, the airplane flight path may be changed and the airplane will deviate from the flight plan. In non-normal, high workload and stressful situations, this required display source switching may also be forgotten, omitted, or delayed. Such scenarios may also represent a very undesirable time for the flight guidance system to revert to an unselected mode.

If the design requires that pilots take an action to inform the system regarding a change in airplane control (PF/PNF), applicants should evaluate and demonstrate the following:

a. If this action causes a mode change in the autoflight system, what are the consequences if the pilots fail to recognize that the flight modes have changed, especially under high workload, stressful and/or abnormal conditions?

b. What are the consequences of the pilots failing to accomplish the switching? The FAA believes that if such action does result in unnecessary changes in the autoflight modes, pilots may be reluctant to perform the necessary switching.

c. Applicants should develop and provide explicit procedures and other information to pilots regarding this action and its consequences. Both test pilots and airplane evaluation group pilots should evaluate these procedures.

Control Labeling

Epic designs may use multifunction control devices which perform different functions under various conditions. Examples include the CCDs, multifunction rotary knobs, multifunction keyboards, and multifunction control and display units (MCDUs). These controls perform a variety of functions, depending on the context. In some designs, certain of these controls are labeled with icons (symbols) in lieu of text. While a limited number of control functions may have icons associated with them that one could reasonably assume the pilot could recognize, most functions have no universally accepted icons. Therefore, the association between the icons and the function controlled would require pilot training and memorization.

§25.1555(a) states the following: "Each cockpit control, other than primary flight controls and controls whose function is obvious, must be plainly marked as to its function and method of operation." Traditionally, "obvious" has been applied to primary flight controls, thrust controls, and fire handles – all other controls are labeled. The intent of this rule is to ensure that pilots can quickly and unambiguously identify the function of every control. In conventional designs, this marking has been accomplished using text, with accompanying symbols in some cases. Using text-labeling formats only, pilots have been able to identify control functions, at an acceptable level of accuracy and consistency.

Part 25, Appendix D, §(c) states that the minimum crew evaluations necessary to show compliance with §25.1523 must consider the kind of operation authorized. The determination of the kind of operation authorized requires consideration of the operating rules under which the airplane will be operated. This consideration includes the nature and extent of the training that the pilots will receive. Furthermore, Appendix D, §(b)(10) requires consideration of an incapacitated pilot in those evaluations.

Use of icons instead of text labeling of controls: In order to show compliance with §25.1555(a) for controls labeled only with icons, the applicant should demonstrate that:

a. The pilot in command (PIC) can, with the minimum requisite training, adequately perform his/her duties at an acceptable level of workload and timeliness, using all functions labeled with icons only, as required by normal, non-normal, and emergency situations. The level of performance should be at least equivalent, in terms of time and accuracy to interpret control function and method of operation, to that which would be expected with text labeling.

b. Since Part 25, Appendix D, §(b)(1), requires consideration of an incapacitated crew member in the determination of compliance with § 25.1523, the applicant should demonstrate that either pilot can safely operate and land the airplane with the other pilot incapacitated, considering the minimum training that each pilot must have. It should be noted that, in some operations, the second in command (SIC) may have significantly less training than the PIC.

Labeling of the Functions Controlled

The applicant should demonstrate that their design provides clear, unambiguous, and quickly and reliably identifiable cues that make the function of the CCD selector switches and multifunction knob obvious, as required by § 25.1555(a). To meet the "obvious" requirement, the applicant should show that a properly trained pilot can rapidly, accurately and consistently identify all control functions. In the context of a CCD, the pilot must be able to quickly and reliably identify what item on the display is “active” as a result of cursor positioning as well as what that function will be performed if the item is selected using the selector buttons and/or changed using the multifunction knob. Pilots must be capable of performing tasks to the same performance standards as would result from the use of conventional controls. The FAA has noted that, in some tests, pilots sometimes have to search for the cursor or may not realize what function is active when operating the multifunction knob. The FAA believes that simply making it possible for the pilots to determine the current function of the selector buttons or the multifunction knob would not satisfy § 25.1555(a), as their functions would not be “obvious". In order to demonstrate compliance with § 25.1555(a), the following should be demonstrated:

a. That pilots will correctly identify and select the control functions, at a speed and error-rate that is equivalent to or better than that of controls that are labeled with text formats. The data required to substantiate that the speed and error rate is equivalent need not be objective data; the applicant may collect subjective data from test subjects to show that the design meets this standard.

b. In order to meet the requirement for "obvious" functioning of the controls, the ability to determine quickly and accurately the function of the selector buttons and the multifunction knob should not require extensive training or experience beyond that which would be expected to be given to a minimally trained SIC pilot. Therefore, evaluations should include subjects that have not been highly trained and practiced in the design. (This constraint does not apply to operation of the control - just to the identification and selection of the current function of the control. Effectiveness of the control for each of the intended functions is covered under § 25.777, and can be based on an assumed level of training.)

Color Coding

The new displays often include very large color pallets. This can lead to problems in the ability to reliably discriminate various elements of the display formats, may introduce color confusion. Applicants should provide a detailed description of their use of colors and should evaluate color selections, considering the guidance provided in AC 25-11, section 5.a,b.

Accessibility of Control and Display Functions

As more and more functions are being controlled using multi-purpose controls (e.g., CCD, MCDU, etc.) and presented on multi-purpose displays, pilots are forced to step through more pages and menus to access functions and information that had previously been immediately accessible using dedicated controls and displays. Convenient access to the various functions can be an important issue. It is crucial that function accessibility of controls and information be evaluated across all flight deck functions, in addition to evaluation on a case-by-case basis. The cumulative effects on workload, task performance times, interference across functions, and crew coordination may be significant.

For each control function, the applicant must show compliance with § 25.777(a), which requires "Each cockpit control must be located to provide convenient operation and to prevent confusion and inadvertent operation." The applicant should consider location within any logic and/or menus in addition to physical location. For overall workload assessments, the applicant should show compliance with § 25.1523, including all of the criteria identified in Appendix D. The applicant should evaluate the accessibility of all flight deck functions. For multipurpose displays, the guidance in AC 25-11, especially section 7.h., should be addressed.

8. Certification Plan

The Epic system certification plan should include, at a minimum, the following items:

a. System description, including Epic configuration definition of all racks, cabinets, modules, software applications and functions.

b. Means for performing airplane level safety assessment.

c. Preliminary system safety assessment for each specific Epic system, including failure, condition classifications, system development assurance levels, hardware design assurance levels and proposed software levels for each function and component.

d. Proposed means and methods of compliance, including service history credit being requested; systems and components previously approved and unchanged, change impact analyses for components changed, EQT previously completed, TSO equipment and non-TSO equipment and functions.

e. Identification of any special conditions, exemptions, deviations, equivalent level of safety proposals.

f. Identification of field-loadable software and who is responsible for loading, modifying, and verifying the software loads.

g. Human factors issues.

h. Software design assurance considerations.

i. Hardware design assurance considerations.

j. Schedule.

EFFECT OF POLICY

The general policy stated in this document is not intended to establish a binding norm; it does not constitute a new regulation and the FAA would not apply or rely upon it as a regulation. The FAA Aircraft Certification Offices (ACO) that certify transport category airplanes should generally attempt to apply this policy, when appropriate; but in determining compliance with certification standards, each ACO has the discretion not to apply these guidelines where it determines that they are inappropriate. However, whenever proposing to deviate from these guidelines, the ACO should generate an issue paper and coordinate it with the Transport Airplane Directorate (TAD) to ensure standardization.

Applicants should expect that the certificating officials will consider this information when making findings of compliance relevant to new certificate actions. Also, as with all advisory material, this statement of policy identifies one means, but not the only means, of compliance.

Questions regarding this guidance should be directed to Ms. Connie Beane, Standardization Branch, ANM-113, telephone 425-227-2796, fax 425-227-1149.

/s/ Ali Bahrami for Vi L. Lipski
Vi L. Lipski,
Manager, Transport Airplane Directorate, ANM-100

Distribution:
All Managers, Aircraft Certification Offices
Manager, Aircraft Engineering Division, AIR-100
Manager, Airplane and Flight Crew Interface Branch, ANM-111
Manager, Standardization Branch, ANM-113
Manager, International Branch, ANM-116

APPENDIX A

Related Guidance Material

Advisory Circulars:

AC 20-115B	RTCA, Inc. Document RTCA/DO-178B, dated January 11, 1993
AC 25.1309-1A	System Design and Analysis, dated June 21, 1988
AC 25-11	Transport Category Airplane Electronic Display Systems, dated July 16, 1987
AC 21-33	Quality Assurance of Software Used in Aircraft and Related Products, dated February 3, 1993
AC 21-35	Computer Generated/Stored Records, dated June 4, 1993
AC 21-36	Quality Assurance Controls for Product Acceptance Software Dated August 11, 1993

FAA Notices:

8110.85	Guidelines for the Oversight of Software Change Impact Analyses used to Classify Software Changes as Major or Minor
8110.86	Guidelines for Software Conformity Inspection and Software Conformity Review
8110.87	Guidelines for Determining the Level of Federal Aviation Administration (FAA) Involvement in Software Projects
8110.90	Guidelines for the Software Review Process
8110.91	Guidelines for the Qualification of Software Tools Using RTCA DO-178B
8110.93	Guidelines for the Approval of Field-Loadable Software by Finding Identicality Through the Parts Manufacturer Approval Process
8110.94	Guidelines for the Approval of Airborne Systems and Equipment Containing User-Modifiable Software
8110.95	Guidelines for the Approval of Field-Loadable Software

RTCA Documents:

RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certification, dated December 1, 1992
RTCA/DO-254	Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000

SAE Documents:

ARP4754	Certification Considerations for Highly-Integrated or Complex Aircraft Systems, dated November 1996
ARP4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, dated December 1996

APPENDIX B

Honeywell Primus Epic
List of Generic Equipment and Software

Epic Components	Likely changed between programs?	Likely degree of change between programs	Comments
MAU:			
Chassis Module Configuration	Yes (see comment)	Significant chassis changes between programs	Only differences are number of slots and one or two channels per MAU
Power Supply Module	NO*	Insignificant	
Network Interface Control Module	NO*	Insignificant	
Processor Module	NO*	Insignificant	
Generic I/O Module (single slot)	NO*	Insignificant	
Generic I/O Module (dual slot)	NO*	Insignificant	
Custom I/O Module	Yes (see comment)	Up to significant (see comment)	Processing h/w is identical to I/O; differences per program are I/O customized to each aircraft
Custom I/O Module	NO*	Insignificant	
Database Module	NO*	Insignificant	
Central Maint. Computer Module	NO*	Insignificant	
GPS Module	NO*	Insignificant	
AFCS I/O Module	NO* (except Augusta)	Insignificant (see comment)	All fixed wing applications plan to use the same hardware; the helicopter version is different.
Flight Control Module	NO*	Insignificant	
Advanced Graphics Module	NO*	Insignificant	
EGPWS Module	NO*	Insignificant	

DU-1080 Display Unit	NO*	Insignificant	
DU-1310 Display Unit	NO*	Insignificant	
Cursor Control Device	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (different CCD types are used on programs
Multi-function Control Display Unit	NO*	Insignificant	
Modular Radio Cabinet:			
MRC Chassis	NO*	Insignificant	
Network Interface Modular	Yes (see comment)	Relatively insignificant (see comment)	Insignificant changes between units of the same model types (two different models exist on the Epic programs)
RF Modules	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (COM and NAV modules will be replaced by VDR and VIDL modules on some of the programs)
Audio Panel	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (several different models exist on the Epic programs)
Radio Altimeter	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (several different models exist on the Epic programs)
Data Mgmt Unit Loader	NO*	Insignificant	
IRS	NO*	Insignificant	
Air Data Module	NO*	Insignificant	

Air Data Probes	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (two different models exist on the Epic program)
Smart Servos	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (several different models exist on the Epic programs)
TCAS	NO*	Insignificant	
Core Software:			
DEOS	NO*	Insignificant	Software and hardware host are expected to be the same between programs
Period Device Driver	NO*	Insignificant	
LAN Device Driver	NO*	Insignificant	
File System	NO*	Insignificant	
Boot	NO*	Insignificant	Boot software is not field loadable.
Core BIT	NO*	Insignificant	
Fault History Manager	NO*	Insignificant	
NIC Application Software	NO*	Insignificant	
System Configuration Monitoring	NO*	Insignificant	
Central Data Loader	NO*	Insignificant	
I/O Software:			
Generic I/O Application Software	NO*	Insignificant	
Custom I/O Application Software	Yes (see comment)	Up to significant (see comment)	New software handling processes are required when new types of I/O are encountered between programs

Central I/O Software	Yes (see comment)	Should be relatively insignificant unless additional Control I/O are created (see comment)	There is currently a study looking at another version of Control I/O module.
Displays Core Software:			
DU-1080 Core Graphics Software	NO*	Insignificant	
ADM Core Graphics Software	NO*	Insignificant	
MCDU Software	NO*	Insignificant	
MRC Software:			
NIM Software (NIC Processor)	NO*	Insignificant	
NIM Software (MRC Processor)	Yes (see comment)	Relatively Insignificant	Two different versions of NIMs are planned for Epic programs. Software changes between the two should be relatively insignificant.
RF Module Software	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (Com and NAV modules will be replaced by VDR and VIDL modules on some of the programs)
Audio Panel Software	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (two different models of audio panels are planned for Epic programs)
Function Software:			
CMC Software	NO*	Insignificant	
AFCS Application Software (incl. Autothrottle, Stall Warning Protection and AFCS I/O)	Yes	Significant	

FMS Application Software	Yes	Up to Significant	
Graphics Generation Software	Yes	Significant	Will be field loadable.
Flight Control Module Software	Yes	Up to Significant	
EGPWS	NO*	Insignificant	
COM Mgmt Unit Software	NO*	Insignificant	
Display Control Software	Yes	Significant	
Monitor/Warning Software	Yes	Significant	
IRS Software	NO*	Insignificant	
ADM Software	NO*	Insignificant	
Air Data Software	NO*	Insignificant	
ASCB-D Data Contents	Yes (see comment)	Up to Significant	Insignificant from the ASCB function and architecture standpoints.
Air Data Probe Software	Yes (see comment)	Significant (see comment)	Insignificant changes between units of the same model types (two different models of probes are planned for the Epic programs)
Smart Servos Software	Yes (see comment)	Relatively Insignificant (see comment)	Insignificant changes between units of the same model types (different models of the servos are planned)
TCAS Software	NO*	Insignificant	
GPS Software	NO*	Insignificant	

Note: *These items are currently planned to be identical across Epic programs. Over time improvements are likely to be made to these items. Due to the timeframe, differences of the various certification programs and follow-on certifications, this may result in upgraded versions of these items to be included in some of the programs but not others.

APPENDIX C

Generic Issue Papers

Software Levels:

ISSUE PAPER

PROJECT: <APPLICANT COMPANY NAME> <PRODUCT NAME & MODEL> <PROJECT NUMBER>	**ITEM:** S-x **STAGE:** 2
REG.REF.: §§ 21.16, 25.1301, 25.1309	**DATE:**
NATIONAL POLICY REF.: AC 20-115B, AC 25.1309-1A	**ISSUE STATUS:** OPEN
SUBJECT: Software Level	**BRANCH ACTION:**
Based on GIP # S-x6b	**COMPLIANCE TARGET:** Pre-TC/STC/ATC/TSOA

ACCEPTABLE MEANS OF COMPLIANCE

STATEMENT OF ISSUE:

The <APPLICANT COMPANY NAME> <PRODUCT NAME & MODEL> will be certificated with digital microprocessor based systems and equipment containing software. Guidance for determining the software level of the embedded software is provided in RTCA document DO-178B. Some systems on the <Aircraft Model> will not utilize DO-178B but will have "critical" or "essential" functions, that is, functions whose failure could cause or contribute to a catastrophic, hazardous severe/major or major failure condition category. While prior guidelines define software development commensurate with such functions, they do not provide requirements for determining the specific software level to be used in a given software application. Furthermore, software errors or malfunctions may cause or contribute to a failure of a system or interfacing systems which are more hazardous than a failure of the system in which the software resides.

BACKGROUND:

RTCA Special Committee 167 produced DO-178B, which addresses the issue of software level assignment. Prior to DO-178B, past practice in the certification of digital systems has been to assign DO-178A criticality levels to software based on the perceived criticality level of the system in which it resides, i.e., systems which by failure analysis (or engineering judgment) were determined to have non-essential functions were developed with non-essential level (Level 3) software. This practice has been shown, in several cases, to allow assignment of software levels lower than is warranted by the actual hazards software errors can produce.

FAA POSITION:

For each system containing software, the applicant shall conduct a systems safety assessment to determine the appropriate software level(s) according to RTCA DO-178B or other acceptable means. For those previously developed systems which did not use DO-178B, the existing methods used in determining software levels may not adequately address the safety requirements for digital airborne systems and equipment. Therefore, the following shall be used in determining software levels to which <Product Name & Model> software will be developed:

> **Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the airplane must be developed and assessed to the guidance of DO-178B Level A or equivalent.**
>
> **Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a hazardous/severe-major failure condition for the airplane must be developed and assessed to the guidance of DO-178B Level B or equivalent.**
>
> **Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a major failure condition for the airplane must be developed and assessed to the guidance of DO-178B Level C or equivalent.**
>
> **Software whose anomalous behavior, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a minor failure condition for the airplane must be developed and assessed to the guidance of DO-178B Level D or equivalent.**
>
> **Software must be developed to the guidance of DO-178B Level A or equivalent if the applicant cannot justify a lower software level.**
>
> Advisory Circular 25.1309-1A and DO-178B provide definitions and guidance for categorizing failure conditions and for conducting the system safety assessment process and providing system safety analyses. Definitions for Catastrophic, Hazardous/Severe-Major, and Major Failure Conditions are provided below for convenience.:
>
> <u>Catastrophic Failure Conditions.</u> Failure conditions which would prevent the continued safe flight and landing of the airplane.

Hazardous/Severe-Major Failure Conditions. Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be:

(1) a large reduction in safety margins or functional capabilities,

(2) physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or

(3) adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.

Major Failure Conditions. Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.

FCAA POSITION:

APPLICANT POSITION:

CONCLUSION:

____ ______________
Manager, Transport Airplane Directorate Date
Airplane Certification

CONTACTS:

TITLE	NAME	INITIALS DATE	PHONE
Originator			
Project Manager			
Project Officer:			
Tech. Specialist	W. Struck		(425) 227-2764

User-Modifiable Software:

ISSUE PAPER

PROJECT: <Applicant Company Name> <Model Number> Project No. <Number>	**ITEM:** S-X **STAGE:** 2 **DATE:**
REG. REF.: §§ FAR 21, 25.1301, 25.1309	**ISSUE STATUS:** Open
NATIONAL POLICY REF.: AC 20-115B, AC 25.1309-1A, Notices 8110.84, 8110.94	**BRANCH ACTION:** ANM-111, ANM-112, ANM-113, ANM-114, ANM-115, ANM-116, ACO, AEG
SUBJECT: Guidance for User-Modifiable Software Used in Airborne Systems	**COMPLIANCE TARGET:** Pre-TC, STC, ATC, TSOA

Based on GIP # S-x4a

ACCEPTABLE MEANS OF COMPLIANCE

STATEMENT OF ISSUE:

The <Applicant Company Name> <Aircraft Model Number> to be certificated may contain User-Modifiable Software. Currently, there is limited FAA policy or guidance for the certification of airborne systems which use user-modifiable software. RTCA document DO-178B provides some guidance for user-modifiable software and FAA notice 8110.94, “Guidelines for the Approval of the Approval of Airborne Systems and Equipment Containing User-Modifiable Software” contains additional criteria and guidance.

The purpose of this Issue Paper is to identify the guidance and criteria to be applied for the approval of user-modifiable software installed on the <Applicant Company Name> <Aircraft Model Number> aircraft.

BACKGROUND:

For this discussion, user-modifiable software is software intended to be modified by the airplane operator without any review or approval by the certification authority, the airframe manufacturer or the system/equipment vendor, that is, an amended type certificate (ATC) or supplemental type certificate (STC) or other approval is not required for its use following modification. Modifications by the user may include modifications to data, to executable code, or to both, so long as the modifications are performed as approved for the system and the guidance and objectives of RTCA DO-178B (or equivalent means), the notice and this Issue Paper are satisfied.

Prior versions of RTCA DO-178 did not address user-modifiable software issues. DO-178B addresses some of the issues with definitions and guidance for user- modifiable software in Sections 2.4 and 5.2.3. However, not all certification and operational issues of user-modifiable software in airborne systems and equipment are addressed by DO-178B. In 1999, the FAA developed Notice 8110.84 (which was re-issued in 2001 as 8110.94) to address these shortcomings, which provided additional guidance for the approval of user-modifiable software.

FAA POSITION:

1. In order to show compliance with §25.1301 and §25.1309 (a), and (b), and secure approval for the installation of systems containing user-modifiable software, the applicant should establish that the user-modifiable software components and all affected aspects of the non-modifiable software components comply with the applicable requirements and objectives of RTCA DO-178B and the FAA Notice 8110.94 (even after it expires).
2. The applicant (or system developer) should identify their plans for addressing the guidance and criteria of DO-178B and Notice 8110.94 in their Plan for Software Aspects of Certification (PSAC, section 11.1 of DO-178B) for each system with this capability, and should gain approval of the PSAC by the cognizant ACO (or FCAA) early in the program.
3. The applicant (or system developer) should summarize their results which demonstrate compliance with the guidance and criteria of DO-178B and Notice 8110.94 in their Software Accomplishment Summary (SAS, section 11.20 of DO-178B) for each system with this capability.
4. Procedures and tools used to install the user-modifiable software should be identified in the System or Software Configuration Index (SCI) for each system and in the appropriate installation manuals, maintenance manuals and/or operations manuals. Tools used to make the modifications may need to be qualified to the guidance of DO-178B, section 12.2.

FCAA POSITION (if applicable):

APPLICANT POSITION:

CONCLUSION:

______________________________________ ______________________

Transport Airplane Directorate Date
Aircraft Certification Service

CONTACTS:

TITLE	NAME	PHONE
Paper Originator	Will Struck	425-227-2764
Project Manager		
Project Officer		

Commercial Off-The-Shelf Software:

ISSUE PAPER

PROJECT: <Applicant Company Name> Model XYZ	**ITEM:** S-x **STAGE:** 2
REG.REF.: §§ FAR 25.1301, 25.1309	**DATE:**
NATIONAL **POLICY REF.:** AC 20-115B, 25-1309-1A	**ISSUE STATUS:** OPEN
SUBJECT: Use of Commercial Off The Shelf (COTS) Software in Aircraft Avionics Systems	**BRANCH ACTION:** Systems-Software and Electrical, Powerplant, Flight Test, MIDO, AEG
Based on GIP # S-x7b	**COMPLIANCE** **TARGET:** Pre-TC, STC, ATC, TSOA

ACCEPTABLE MEANS OF COMPLIANCE

STATEMENT OF ISSUE:

The <Applicant> Model <Number> will be certificated with digital microprocessor based systems installed which may contain commercial off-the-shelf (COTS) software. This issue paper identifies acceptable means of certifying airborne systems and equipment containing COTS software.

BACKGROUND:

Many COTS software applications and components have been developed for use outside the field of commercial air transportation. Much of this COTS software has been developed for systems for which safety is not a concern, or for systems with safety criteria different from that of commercial transport airplanes. Consequently, for COTS software, adequate artifacts may not be available to assess the adequacy of the software integrity. Available evidence may be insufficient to show that adequate software life cycle processes were used. RTCA document DO-178B recognizes the above, and addresses means by which COTS may be shown to comply with transport airplane certification requirements.

FAA POSITION:

RTCA document DO-178B provides a means for obtaining the approval of airborne COTS software. For those systems which make use of COTS software, the objectives of DO-178B should be satisfied. If deficiencies exist in the life cycle data of COTS software, DO-178B addresses means to augment that data to satisfy the objectives. If the applicant chooses to utilize a means other than DO-178B, the applicant should propose in their Plan for Software Aspects of Certification, how they intend to show that all COTS software complies with §§ 25.1301 and 25.1309 and the guidance of DO-178B. The applicant should obtain agreement on the means of compliance for COTS software from the FAA ACO (or FCAA) prior to implementation.

FCAA POSITION:

APPLICANT POSITION:

CONCLUSION:

_________________________________ ____________

Manager, Transport Airplane Directorate Date
Airplane Certification

CONTACTS:

TITLE	NAME	INITIALS DATE	PHONE
Originator			
Project Manager			
Project Officer:			
Tech. Specialist	Will Struck		(425) 227-2764

Programmed Logic Devices:

ISSUE PAPER

PROJECT: <COMPANY NAME>
<PRODUCT NAME & MODEL>
<PROJECT NUMBER>

ITEM: S-x

STAGE: 2

REG.REF.: §§ 21.16, 25.1301, 25.1309

DATE:

NATIONAL POLICY REF.: AC 25-1309-1A, AC 20-115B

ISSUE STATUS: OPEN

SUBJECT: Programmed Logic Devices

BRANCH ACTION:

Based on GIP # S-x1b

COMPLIANCE TARGET:
Pre-TC/STC/ATC/TSOA

ACCEPTABLE MEANS OF COMPLIANCE

STATEMENT OF ISSUE:

The <COMPANY NAME> <PRODUCT NAME & MODEL> proposes to use Programmed Logic Devices in airborne systems and equipment. At present there is no specific FAA policy or guidance for certification of airborne systems containing Programmed Logic Devices. The purpose of this Issue Paper is to define the specific aspects of certification associated with PLDs for systems containing such devices on the <COMPANY NAME> <PRODUCT NAME & MODEL> program.

BACKGROUND:

Systems used on the <Aircraft Model Product> will include Programmed Logic Devices. For clarification the following terminology applies:

Programmed Logic Devices
Programmed Logic Devices include Application Specific Integrated Circuits (ASIC) and Programmable Logic Devices (PLDs).

ASIC
An ASIC is defined as any masked programmed integrated circuit that is developed by or for <COMPANY NAME> <Product Name & Model> that requires physical customization of the device die by an ASIC vendor. Gate array, cell based and custom

designs are included as they involve some level of customization of the mask sets used in the fabrication of the devices.

PLD
A PLD is defined as any device that is purchased as an electronic part and altered to perform an application specific function. PLDs include, but are not limited to, Programmable Array Logic (PAL) devices, Programmable Logic Array (PLA) devices, General Array Logic (GAL) devices, Field Programmable Gate Array (FPGA) devices, and Erasable Programmable Logic Devices (EPLD). Programmable Logic Devices typically require programming by software which is done in-house by the equipment manufacturer.

These devices will be used in systems which have functions that can affect the safety of the airplane. These devices are often as complex as software controlled microprocessor-based systems. Because of the nature and complexity of systems containing digital logic, the FAA has determined that adherence to a structured approach may be used to show compliance with FAR 25.1309 for complex, programmable logic devices. Although systems containing programmed logic devices can perform functions of the same complexity as software based systems, the FAA has no policy or guidelines for certification of systems containing programmed logic devices. However, the challenges of assuring software and programmed logic device design logic are essentially the same. One means of showing such compliance for complex, programmable logic devices is adherence to the guidelines of RTCA document DO-254, "Design Assurance Guidance for Airborne Electronic Hardware." This issue paper is concerned with the assurance of the encoded logic embedded in these devices.

FAA POSITION:

There is no existing FAA policy or guidance for showing compliance to the existing rules for those aspects of certification associated with Programmed Logic Devices. Accordingly, certification of systems on the <COMPANY NAME> <PRODUCT NAME & MODEL> which contain such devices should achieve the following:

Programmed Logic Devices associated with functions whose failure or malfunction could cause or contribute to a catastrophic failure condition for the aircraft as defined in Advisory Circular 25.1309-1A or to a hazardous/severe-major failure condition as defined in RTCA document DO-254, should undergo testing and deterministic analysis which demonstrates correct operation under all combinations and permutations of conditions of the gates within the device.

Programmed Logic Devices associated with functions whose failure or malfunction could cause or contribute to a major condition for the aircraft as defined in Advisory Circular 25-1309-1A should undergo testing and deterministic analysis which demonstrates correct operation under all combinations and permutations of conditions at the pins of the device.

In the event that the complexity of the device makes the testing and analysis requirements outlined above unfeasible, the following applies:

> **Programmed Logic Devices should be developed using a structured development approach approved by the FAA (and FCAA, if applicable). The structured approach should provide design assurance rigor which is commensurate with the hazard associated with failure or malfunction of the system in which the Programmed Logic Device is located and its function within those systems. Guidance in this area can be found in DO-254 which describes hardware design assurance level determination; and the applicable guidance for each level.**
>
> **Furthermore, the applicant should ensure that:**
> **1) Programmed Logic Devices are identified in the certification plans,**
> **2) The PLD design assurance strategy and rigor for each device is acceptable to the FAA (and, if applicable, FCAA), and**
> **3) Accomplishment summaries describe the means and level of design assurance achieved.**

Information on how the applicant intends to present certification data for Programmed Logic Devices can be included in current certification plan documents or as stand-alone plans for Programmed Logic Devices.

If the applicant is planning on using the guidance of DO-254, they should identify each PLD to be used in their product, and specify any architectural and/or mitigation techniques to be used, hardware design assurance levels, rationale for each PLD's level assignment, and design assurance strategy in their certification plans and get approval from the FAA ACO (or FCAA for validation projects).

Guidance identified in this issue paper does not in any way alleviate the need for traditional methods for hardware design and assurance.

The guidance of this issue paper is applicable to PLD's used in all electrical, electronic, and electro-mechanical systems and equipment used for avionics, flight controls, fuel systems, landing gear, doors, power plant, propulsion, structures, environmental, and TSO systems and equipment.

FCAA POSITION:

APPLICANT POSITION:

CONCLUSION:

____________________________ ____________

Manager, Transport Airplane Directorate Date
Airplane Certification

CONTACTS:

TITLE	NAME	INITIALS DATE	PHONE
Originator			
Project Manager			
Project Officer:			
Tech. Specialist	Forrest Keller		(425) 227-xxxx

APPENDIX D

Acronyms

ABC	assembly branch coverage
AC	advisory circular
A/C	aircraft
ACO	Aircraft Certification Office
ADM	air data module
AFCS	auto-flight control system
ALT	altitude
APU	auxiliary power unit
ARP	aerospace recommended practices
ASIC	application specific integrated circuit
ASTC	amended supplemental type certificate
ATC	amended type certificate
BIT	built-in test
CCD	cursor control device
CFR	Code of Federal Regulations
CHG	change
CMC	central maintenance computer
COTS	commercial off-the-shelf
CRM	crew resource management
DEOS	digital engine operating system
DU	display unit
EGPWS	enhanced ground proximity warning system
EQT	environmental qualification testing
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FHA	functional hazard assessment
FMS	flight management system
FPGA	field programmable gate array
GPS	global positioning system
HDG	heading
HIRF	high-intensity radiated fields
I/O	input/output
IRS	inertial reference system
LAN	local area network
LNAV	lateral navigation
LVL	level
MAU	modular avionics unit
MC/DC	modified condition decision coverage
MCDU	multifunction control and display unit
MEL	minimum equipment list

MMEL	master minimum equipment list
MRC	modular radio cabinet
NIC	network interface controller
NIM	network interface module
PF	pilot flying
PIC	pilot in command
PLD	programmable logic device
PNF	pilot not flying
RF	radio frequency
SAE	The Engineering Society for Advancing Mobility Land, Sea, Air and Space (formerly Society of Automotive Engineers)
SIC	second in command
STC	supplemental type certificate
TAD	Transport Airplane Directorate
TC	type certificate
TCAS	traffic alert collision avoidance system
TSO	technical standard order
TSOA	technical standard order authorization
VNAV	vertical navigation